IN THE CLAIMS

1. (currently amended) A data processing method performed by ~~means~~a device to be authenticated and an authenticating ~~means~~device, the ~~means~~ device to be authenticated holding first authentication use data generated by encryption using key data and the authenticating device ~~means~~ holding the key data, the method comprising:

generating a first random value at the device to be authenticated;

encrypting the first random value at the device to be authenticated using a first encryption process and the first authentication use data;

providing key designation data designating the key data and the encrypted first random value from the ~~means~~ device to be authenticated to the authenticating device~~means~~;

obtaining the key data at the authenticating device using the key designation data;

performing encryption at the authenticating ~~means~~device using the ~~designated~~ key data to generate second authentication use data;

decrypting the encrypted first random value at the authenticating device using the first encryption process and the second authentication use data to obtain the first random value;

encrypting the first random value at the authenticating device using a second encryption process and the second authentication use data to generate a further encrypted value;

providing the further encrypted value from the authenticating device the device to be authenticated;

decrypting the further encrypted value at the device to be authenticated using the second encryption process and the first authentication use data;

comparing the decrypted further encrypted value ~~first authentication use data~~ with the first random value~~second authentication use data~~ at the device to be authenticated; and

executing processing related to the key data in the authenticating ~~means~~device ~~when~~ in response to the comparing~~son~~ step determining~~es~~ that the decrypted further encrypted value and the first random value are the same thereby indicating that the first authentication use data and the second authentication use data are the same.

2. (currently amended) A data processing system, comprising:

a ~~means~~ device to be authenticated for holding first authentication use data generated by encryption using key data; and

an authenticating device ~~means~~ for holding the key data;~~,~~

wherein the ~~means~~ device to be authenticated generates a first random value, encrypts the first random value using a first encryption process and the first authentication use data, and provides key designation data designating the key data and the encrypted first random value to the device to be authenticat~~ing~~ed ~~means~~,

the authenticated~~ing~~ device ~~means~~ obtains the key data using the key designation data, performs encryption using the ~~designated~~ key data to generate second authentication use data, decrypts the encrypted first random value using the first encryption process and the second authentication use data to obtain the first random value, encrypts the first random value using a second encryption process and

the second authentication use data to generate a further encrypted value, and provides the further encrypted value to the authenticating device,

the ~~means~~ device to be authenticated decrypting the further encrypted value ~~uses~~ using the second encryption process and the first authentication use data, and compares the decrypted further encrypted value with the first random value~~for authentication and the authenticating means uses the second authentication use data for authentication~~, and

the authenticating ~~means~~device executes processing related to the key data ~~when~~ in response to the determining that the decrypted further encrypted value and the first random value are the same thereby indicating that the first authentication use data and the second authentication use data are the same.

3. (currently amended) A data processing method in which an authenticating ~~means~~ device holding predetermined key data performs an authentication process together with a ~~means~~ device to be authenticated holding first authentication use data generated by encryption using the key data, the method comprising:

receiving key designation data for designating the key data from the ~~means~~ device to be authenticated;

generating second authentication use data by encryption using the designated key data;

generating a random value;

encrypting the generated random value using a first encryption process and the second authentication use data;

providing the encrypted random value to the device to be authenticated, the device to be authenticated decrypting the encrypted random value using the first encryption process and the first authentication use data to obtain the generated random value, and encrypting the generated random

value at the device to be authenticated using a second encryption process and the first authentication use data to generate a further encrypted value;

receiving the further encrypted value from the device to be authenticated;

decrypting the further encrypted value using the second encryption process and the second authentication use data;

comparing the decrypted further encrypted value ~~second authentication use data~~ with the generated random value~~first authentication use data~~; and

executing processing related to the key data ~~when~~ in response to the comparing~~son~~ step determines that the decrypted further encrypted value and the generated random value are the same thereby indicating that the first authentication use data and the second authentication use data are the same.

4. (currently amended) The ~~A~~ data processing method as set forth in claim 3, wherein the executing step includes executing ~~the~~ functions of the authenticating ~~means~~device authorized to the ~~means~~device to be authenticated related to the key data or accessing ~~the~~ data held by the authenticating ~~means~~device.

5. (currently amended) The ~~A~~ data processing method as set forth in claim 3, wherein ~~the generating step includes generating~~ the second authentication use data is generated using a plurality of different key data, and the executing step includes executing a plurality of processing~~s~~ steps related to the plurality of different key data.

6. (currently amended) The ~~A~~ data processing method as set forth in claim 5, wherein the executing step includes executing a plurality of processing~~s~~ steps including ~~the~~ functions of the authenticating ~~means~~device and accessing ~~the~~

data held by the authenticating ~~means~~device relating to the plurality of different key data.

7. (currently amended) The ~~A~~ data processing method as set forth in claim 3, wherein the executing step includes accessing ~~the~~ a plurality of data modules related to single key data when the authenticating ~~means~~device holds a plurality of data modules as data.

8. (currently amended) The ~~A~~ data processing method as set forth in claim 3, ~~wherein the receiving step includes receiving~~ further comprising reading the key designation data ~~read~~ by a device of the ~~means~~ device to be authenticated from an integrated circuit holding the first authentication use data and the key designation data.

9. (currently amended) The ~~A~~ data processing method as set forth in claim 3, wherein the first authentication use data is data generated by encrypting predetermined data using the key data.

10. (currently amended) The ~~A~~ data processing method as set forth in claim 9, wherein the first authentication use data is data generated by encrypting data obtained by encrypting the predetermined data using the key data by further using tamper-proofing key data managed by the ~~means~~device to be authenticated.

11. (currently amended) A data processing system holding predetermined key data for use in an authentication process with a ~~means~~device to be authenticated holding first authentication use data generated by encryption using the key data, the data processing system comprising:

inputting means for inputting key designation data for designating the key data from the ~~means~~ device to be authenticated;

~~authenticating~~ means for generating second authentication use data by encryption using the designated key data; ~~and~~

means for generating a random value;

means for encrypting the generated random value using a first encryption process and the second authentication use data;

means for providing the encrypted random value to the device to be authenticated, the device to be authenticated decrypting the encrypted random value using the first encryption process and the first authentication use data to obtain the generated random value, and encrypting the generated random value at the device to be authenticated using a second encryption process and the first authentication use data to generate a further encrypted value;

means for receiving the further encrypted value from the device to be authenticated;

means for decrypting the further encrypted value using the second encryption process and the second authentication use data;

means for comparing the decrypted further encrypted value ~~second authentication use data~~ with the generated random value~~first authentication use data~~; and

~~controlling~~ means for executing processing related to the key data ~~when the comparison by~~ in response to the ~~authenticating~~ means for comparing determininges that the decrypted further encrypted value and the generated random value are the same thereby indicating that the first authentication use data and the second authentication use data are the same.

12. (currently amended) A computer-readable medium having stored therein a computer-readable program having instructions

for ~~causing~~ executing a data processing ~~system~~ method in which an authenticating device holding predetermined key data ~~to execute~~ performs an authentication process with a ~~means~~ device to be authenticating~~ed~~ holding first authentication use data generated by encryption using the key data, the ~~authentication process~~ method comprising:

receiving key designation data for designating the key data from the ~~means~~device to be authenticated;

generating second authentication use data by encryption using the designated key data;

generating a random value;

encrypting the generated random value using a first encryption process and the second authentication use data;

providing the encrypted random value to the device to be authenticated, the device to be authenticated decrypting the encrypted random value using the first encryption process and the first authentication use data to obtain the generated random value, and encrypting the generated random value at the device to be authenticated using a second encryption process and the first authentication use data to generate a further encrypted value;

receiving the further encrypted value from the device to be authenticated;

decrypting the further encrypted value using the second encryption process and the second authentication use data;

comparing the decrypted further encrypted value ~~second authentication use data~~ with the generated random value~~first authentication use data~~; and

executing processing related to the key data ~~when~~ in response to the comparing~~son~~ step determines that the decrypted further encrypted value and the generated random value are the same thereby indicating that the first

authentication use data and the second authentication use data are the same.

13. (currently amended) A data processing method performed by a ~~means~~ device to be authenticated, the ~~means~~ device to be authenticated holding first authentication use data generated by encryption using key data, an authentication device holding the key data, the method comprising:

generating a first random value;

encrypting the first random value using a first encryption process and the first authentication use data;

providing key designation data designating the key data and the encrypted first random value ~~used to generate the first authentication use data~~ to the authenticating device~~means~~, the authenticating ~~means~~ device obtaining the key data using the designated key data, performing encryption using the key data to generate second authentication use data, decrypting the encrypted first random value using the first encryption process and the second authentication use data to obtain the first random value, and encrypting the first random value using a second encryption process and the second authentication use data to generate a further encrypted value;

receiving the further encrypted value from the authenticating device;

decrypting the further encrypted value using the second encryption process and the first authentication use data;

comparing the decrypted further encrypted value with the first random value~~using the first authentication use data in an authentication process in which the authenticating means uses the second authentication use data~~; and

causing the authenticating ~~means~~ device to execute processing related to the key data in response to the comparing step determining that the decrypted further encrypted value and the first random value are the same thereby indicating that the first authentication use data and the second authentication use data are the same~~based on the results of the authentication process~~.

14. (currently amended) The ~~A~~ data processing method as set forth in claim 13, wherein the ~~means~~ device to be authenticated reads and holds the first authentication use data and the key designation data from a predetermined integrated circuit.

15. (currently amended) The ~~A~~ data processing method as set forth in claim 13, wherein the ~~causing~~ executing step includes causing the authenticating ~~means~~device to execute ~~the~~ functions of the authenticating ~~means~~device authorized to the ~~means~~device to be authenticated related to the key data or accessing ~~the~~ data held by the authenticating ~~means~~device.

16. (currently amended) The ~~A~~ data processing method as set forth in claim 13, wherein the authenticating ~~means~~device includes a plurality of authenticating ~~means~~devices, ~~the providing step includes collectively providing the key designation data to the plurality of authenticating means,~~ and the ~~causing~~ executing step includes collectively causing the plurality of authenticating means to ~~perform the~~ execute processing~~s~~ related to the key data.

17. (currently amended) The ~~A~~ data processing method as set forth in claim 13, further comprising providing a screen displaying an image corresponding to the authenticating ~~means~~device for performing the processing by using a plurality of different patterns in accordance with an operation state of the authenticating ~~means~~device.

18. (currently amended) The ~~A~~ data processing method as set forth in claim 17, wherein the screen providing step includes providing a screen displaying an image corresponding to the authenticating ~~means~~device by a pattern enabling determination of whether the authenticating ~~means~~device has confirmed the authenticity of the ~~means~~device to be authenticated by the authentication process.

19. (currently amended) A data processing system holding first authentication use data generated by encryption using key data, the first authentication use data being for use in an authentication process with an authenticating device~~means~~, the authenticating device holding the key data, the data processing system comprising:

means for generating a first random value;

means for encrypting the first random value using a first encryption process and the first authentication use data;

means for providing key designation data designating the key data and the encrypted first random value ~~used to generate the first authentication use data~~ to the authenticating device~~means~~, the authenticating ~~means~~ device obtaining the key data using the designated key data, performing encryption using the key data to generate second authentication use data, decrypting the encrypted first random value using the first encryption process and the second authentication use data to obtain the first random value, and encrypting the first random value using a second encryption process and the second authentication use data to generate a further encrypted value;

means for receiving the further encrypted value from the authenticating device;

means for decrypting the further encrypted value using the second encryption process and the first authentication use data;

means for comparing the decrypted further encrypted value with the first random value~~using the first authentication use data in an authentication process in which the authenticating means uses the second authentication use data~~; and

means for causing the authenticating device ~~means~~ to executinge processing related to the key data in response to the comparing step determining that the decrypted further encrypted value and the first random value are the same thereby indicating that the first authentication use data and the second authentication use data are the same~~based on the results of the authentication process~~.

20. (currently amended) A computer-readable medium having stored therein a computer-readable program having instructions for ~~causing~~ executing a data processing method in which a data processing system holding first authentication use data generated by encryption using key data ~~to execute~~ performs an authentication process with authenticating device~~means~~, the authenticating device holding the key data, the ~~authentication process~~ method comprising:

generating a first random value;

encrypting the first random value using a first encryption process and the first authentication use data;

providing key designation data designating the key data and the encrypted first random value ~~used to generate the first authentication use data~~ to the authenticating device~~means~~, the authenticating ~~means~~ device obtaining the key data using the designated key data, performing encryption using the key data to generate second authentication use data, decrypting the encrypted first

random value using the first encryption process and the second authentication use data to obtain the first random value, and encrypting the first random value using a second encryption process and the second authentication use data to generate a further encrypted value;

receiving the further encrypted value from the authenticating device;

decrypting the further encrypted value using the second encryption process and the first authentication use data;

comparing the decrypted further encrypted value with the first random value~~using the first authentication use data in a comparison with the second authentication use data~~; and

causing the authenticating ~~means~~device to execute processing related to the key data in response to the comparing step determining that the decrypted further encrypted value and the first random value are the same thereby indicating that the first authentication use data and the second authentication use data are the same~~based on the results of the comparison~~.

21. (new) The data processing method as set forth in claim 1, further comprising:

generating a second random value at the authenticating device;

encrypting the second random value at the authenticating device using a second encryption process and the second authentication use data;

providing the encrypted second random value from the authenticating device to the device to be authenticated;

decrypting the encrypted second random value at the device to be authenticated using the second encryption

process and the first authentication use data to obtain the second random value;

encrypting the second random value at the device to be authenticated using the first encryption process and the first authentication use data to generate a still further encrypted value;

providing the still further encrypted value from the device to be authenticated to the authenticating device;

decrypting the still further encrypted value at the authenticating device using the first encryption process and the second authentication use data; and

comparing the decrypted further encrypted value with the first random value at the authenticating device;

the executing step executing the processing related to the key data in the authenticating device in response to the comparing step at the authenticating device determining that the decrypted further encrypted value and the first random value are the same thereby indicating that the first authentication use data and the second authentication use data are the same.

22. (new) The data processing system as set forth in claim 2, wherein

the authenticating device generates a second random value, encrypts the second random value using a second encryption process and the second authentication use data, and provides the encrypted second random value to the device to be authenticated;

the device to be authenticated decrypts the encrypted second random value using the second encryption process and the first authentication use data to obtain the second random value, encrypts the second random value using the first encryption process and the first authentication use data to generate a still further encrypted value, and

provides the still further encrypted value to the authenticating device;

the authenticating device decrypts the still further encrypted value using the first encryption process and the second authentication use data, and compares the decrypted further encrypted value with the first random value device;

the executing step executing the processing related to the key data in the authenticating device in response to the comparing step at the authenticating device determining that the decrypted further encrypted value and the first random value are the same thereby indicating that the first authentication use data and the second authentication use data are the same.